

**Patent Abstract**

GER 1999-03-11 19737874 **Method about initializing a theft protection system for a motor vehicle**

**ANNOTATED TITLE-** Verfahren zum Initialisieren eines Diebstahlschutzsystems foOr ein Kraftfahrzeug

**INVENTOR-** Lindner, Frank 93105 Tegernheim DE

**INVENTOR-** Rehfeld, Frank 93047 Regensburg DE

**INVENTOR-** Schneider, Christian 93049 Regensburg DE

**APPLICANT-** Siemens AG 80333 MoOnchen DE

**PATENT NUMBER-** 19737874/DE-C1

**PATENT APPLICATION NUMBER-** 19737874

**DATE FILED-** 1997-08-29

**DOCUMENT TYPE-** C1, PATENT SPECIFICATION (FIRST PUBL.)

**PUBLICATION DATE-** 1999-03-11

**INTERNATIONAL PATENT CLASS-** B60R02500; B60R02504; E05B06512; B60R02500; G07C00900E14C

**PATENT APPLICATION PRIORITY-** 19737874, A

**PRIORITY COUNTRY CODE-** DE, Germany, Ged. Rep. of

**PRIORITY DATE-** 1997-08-29

**FILING LANGUAGE-** German

**LANGUAGE-** German NDN- 203-0418-1288-4

By unorthodox operating of a key (3) into the ignition palace (14), the theft protection system is put into the initialization condition. Over a Wegfahrsperr (16), a bidirectional dialogue with the key (3) then takes place. If the dialogue is recognized as justifiable, a start value turns into the key (3) from the Wegfahrsperr on the one hand and transfers from the key to the recipient (11) of the Schlieo"systems (1) on the other hand. The start value turns in the key (3) into generating of a change code and in the recipient (11) to generating a with it to comparative debit codes uses.

**EXEMPLARY CLAIMS-** 1. Method about initializing a theft protection framework for a motor vehicle, with what the theft protection system shows, .: a key (3), on the one Fernbedieneinheit (4, 5, 6, 7) to the Ver -. or Entriegeln of a Zentralverriegelungsanlage (1) and a Transponder (4, 5, 8) to solving a Wegfahrsperr (2) angeordnet is -. a recipient (11) in the motor vehicle, the signals of the Fernbedieneinheit, 4, 5, 6, 7, receives and appraises, and -. one send -. and reception unit (16) at a palace (14), that sends out a request signal to the Transponder (4, 5, 8), an encoded answer signal of the Transponder receives and the answer signal on his/its entitlement pro Oft, gekennzeichnet through following steps: . Introduces of an initialization condition, through what the recipient (11) and this send -. and reception unit (16) is put into an initialization condition -. Sends out of the request signal at the Transponder (4, 5, 8) -. Sends back send of the answer signal at them/her/it -. and reception unit (16) -. Reviewing of the answer signal on his/its entitlement, in that a code information contained in the answer signal with a stored debit code information expected and is compared -. It sends out of an encoded start value at the key (3) if the answer signal was recognized as justifiable, as well as storages of the start value in a storage (5) of the key (3), and -. Refers of the start value of the key (3) at the recipient (11). 2. Method for claim 1, marked by it, that the start value as initially value to generating a coded long-distance bedienwechselcodesignals in a storage (13) of the recipient (11) is stored. 3. Method for one of the preceding claims, marked by it, that a successful initialization is shown by an ad unit acoustically optically und/oder. 4. Method for one of the preceding claims, marked by it, that the signals send between the Transponder (4, 5, 8) and this -. and reception unit (16) as inductive or optical energy -. or

data signals and the signals of the

NÔ-DESCRIPTORS



21 Aktenzeichen: 197 37 874.9-51  
22 Anmeldetag: 29. 8. 97  
43 Offenlegungstag: -  
45 Veröffentlichungstag  
der Patenterteilung: 11. 3. 99

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

73 Patentinhaber:  
Siemens AG, 80333 München, DE

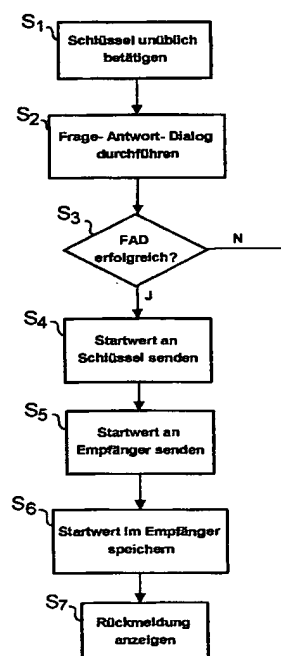
72 Erfinder:  
Lindner, Frank, 93105 Tegernheim, DE; Rehfeld,  
Frank, 93047 Regensburg, DE; Schneider, Christian,  
93049 Regensburg, DE

56 Für die Beurteilung der Patentfähigkeit in Betracht  
gezogene Druckschriften:

DE 1 95 16 992 C2  
DE 44 11 450 C1  
DE 43 02 550 C2  
DE 42 25 221 A1

54 Verfahren zum Initialisieren eines Diebstahlschutzsystems für ein Kraftfahrzeug

57 Durch unübliches Betätigen eines Schlüssels (3) im  
Zündschloß (14) wird das Diebstahlschutzsystem in den  
Initialisierungszustand versetzt. Über eine Wegfahrsperr  
(16) findet dann ein bidirektionaler Dialog mit dem  
Schlüssel (3) statt. Falls der Dialog als berechtigt erkannt  
wird, wird ein Startwert einerseits von der Wegfahrsperr  
zum Schlüssel (3) und andererseits vom Schlüssel zum  
Empfänger (11) des Schließsystems (1) übertragen. Der  
Startwert wird im Schlüssel (3) zum Erzeugen eines  
Wechselcodes und im Empfänger (11) zum Erzeugen ei  
nes damit zu vergleichenden Sollcodes verwendet.



Die Erfindung betrifft ein Verfahren zum Initialisieren eines Diebstahlschutzsystems für ein Kraftfahrzeug, insbesondere zum Initialisieren einer fernbedienbaren Zentralverriegelungsanlage.

Ein bekanntes Diebstahlschutzsystem (DE 43 02 550 C2) weist einen tragbaren Sender auf, der Codesignale zum Fernbedienen der Zentralverriegelungsanlage zu einem Empfänger im Kraftfahrzeug sendet. Die Codesignale sind dabei bei jedem Aussenden gegenüber dem vorherigen Aussenden verändert (Wechselcode oder Rolling Code).

Wenn dieses Diebstahlschutzsystem initialisiert wird, so werden Sender und Empfänger zunächst in einen Initialisierungszustand durch Eingabe eines Sondersignals über eine Diagnoseschnittstelle oder durch unübliches Betätigen des Zündschlüssels verbracht. Anschließend muß der Empfänger ein Codesignal eines bisher berechtigten Senders empfangen, damit die Initialisierung durchgeführt werden kann.

Ein solches Diebstahlschutzsystem kann nur dann nach einem Batteriewechsel initialisiert werden, wenn das zuletzt gültige Codesignal in dem Sender noch gespeichert ist. Hierzu ist ein aufwendiger Speicher notwendig, der zwangsläufig mehr Energie benötigt. Wenn ein einfacher Speicher, wie ein ohnehin vorhandenes RAM, verwendet wird, dann bleibt das zuletzt gültige Codesignal nach einem Batteriewechsel nicht mehr erhalten. Infolgedessen kann kein gültiges Codesignal nach Batteriewechsel ausgesendet werden. Das Diebstahlschutzsystem ist dann nicht zu initialisieren.

Bei einem solchen Diebstahlschutzsystem besteht überdies die Gefahr, daß der Sender bei der Initialisierung zu weit vom Empfänger entfernt ist, so daß der Empfänger den im Schlüssel erzeugten Startwert nicht empfängt. Dann ist zwar der Sender initialisiert, jedoch nicht der Empfänger. Der Sender kann somit die Zentralverriegelungsanlage nicht mehr steuern, da beide nicht mehr "zusammenpassen".

Bei einem weiteren bekannten Diebstahlschutzsystem (DE 44 11 450 C1) werden Einwegfunktionswerte für die Codesicherung fahrzeugseitig gespeichert werden. Das Auslesen der Werte ermöglicht keine unberechtigte Herstellung eines Nachschlüssels und somit keine unberechtigte Initialisierung.

Bei einem anderen Diebstahlschutzsystem (DE 195 16 992 C1) wird ein Aufforderungssignal vom Kraftfahrzeug aus zu einem Transponder gesendet. Das Aufforderungssignal enthält dabei eine Speicheradresse, unter der der Transponder in seinem Speicher ein entsprechendes Codesignal aus liest und zum Kraftfahrzeug zurücksendet.

Bei einem weiteren, bekannten Diebstahlschutzsystem (DE 43 25 221 A1) wird mittels einer bereits gespeicherten Codierung eines Schlüssels eine Speicherbereitschaft aktiviert. Nach Identifizierung des Schlüssels wird von dem Diebstahlschutzsystem ein Mode aktiviert, mittels dem die Codierung von einem weiteren Schlüssel in das Diebstahlschutzsystem eingespeichert wird.

Der Erfindung liegt das Problem zugrunde, ein Verfahren zum Initialisieren eines Diebstahlschutzsystems zu schaffen, bei dem das Diebstahlschutzsystem einfach aufgebaut ist und bei dem ein Initialisieren durch einen Benutzer einfach und zuverlässig durchgeführt werden kann.

Dieses Problem wird erfindungsgemäß durch ein Verfahren mit den Merkmalen von Patentanspruch 1 gelöst. Dabei wird zunächst ein fahrzeugseitiger Empfänger und eine Sende- und Empfangseinheit im Kraftfahrzeug in einen Initialisierungszustand versetzt. Anschließend sendet die Sende- und Empfangseinheit ein Anforderungssignal an einen Transponder auf einem Schlüssel aus, der daraufhin mit

einem Antwortsignal antwortet. Das Antwortsignal wird in der Sende- und Empfangseinheit auf seine Berechtigung überprüft. Falls das Antwortsignal berechtigt ist, so wird ein Startsignal zu dem Schlüssel gesendet und dort gespeichert. Außerdem wird das Startsignal von dem Schlüssel weiter zu dem Empfänger geleitet und dort ebenfalls gespeichert.

Bei diesem Verfahren befindet sich der Schlüssel in unmittelbarer Umgebung des Empfängers. Somit ist weitgehend sichergestellt, daß die bei der Initialisierung ausgesendeten Signale sowohl den Schlüssel als auch den Empfänger erreichen.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen gekennzeichnet. So kann eine erfolgreiche Initialisierung als Rückmeldung an den Benutzer durch eine Anzeigeeinheit optisch oder akustisch angezeigt werden. Die zwischen dem Schlüssel und dem Empfänger übertragenen Signale können optische oder hochfrequente Signale sein. Zwischen dem Schlüssel und der Sende- und Empfangseinheit werden Energie- oder Datensignale induktiv oder optisch übertragen.

Das Einleiten des Initialisierungszustands kann durch unübliches Betätigen des Schlüssels in dem Schloß innerhalb einer vorgegebenen Zeitdauer oder auch durch Anstecken eines externen Geräts an eine Diagnoseschnittstelle und Übertragen eines Initialisierungssignals vorgenommen werden.

Ein Ausführungsbeispiel der Erfindung wird im folgenden anhand der schematischen Zeichnungen näher erläutert. Es zeigen:

**Fig. 1** ein Blockschaltbild eines Diebstahlschutzsystems und

**Fig. 2** ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens zum Initialisieren des Diebstahlschutzsystems nach **Fig. 1**.

Ein Diebstahlschutzsystem für ein Kraftfahrzeug weist eine fernbedienbare Zentralverriegelungsanlage **1** (**Fig. 1**) und eine elektronische Wegfahrsperre **2** auf. Auf einem Griff eines Tür- oder Zündschlüssels **3** ist eine Elektronikereinheit, mit der codierte Signale (im folgenden als Codesignale bezeichnet) zum fernbedienten Ver- oder Entriegeln der Zentralverriegelungsanlage **1** oder codierte Signale (im folgenden als Antwortcodesignale bezeichnet) zum Lösen der Wegfahrsperre **2** drahtlos ausgesendet werden.

Die Elektronikereinheit auf dem Zündschlüssel **3** weist eine zentrale Steuereinheit **4** auf, die mit einem Speicher **5**, insbesondere einem RAM, elektrisch verbunden ist. Die Steuereinheit **4** steuert einen Sender **6**, damit dieser die Codesignale zum Ver- oder Entriegeln von Türschlössern der Zentralverriegelungsanlage **1** über ein Sendeelement **7** aussendet. Ebenso steuert die Steuereinheit **4** einen Schwingkreis **8**, um Energie oder Daten zu empfangen (werden in einem Anforderungssignal übertragen) oder Daten mit einer Codierung auszusenden (werden im Antwortcodesignal moduliert übertragen).

Außerdem ist eine austauschbare Energiequelle, wie z. B. eine Batterie **9**, auf dem Zündschlüssel **3** angeordnet, die die Bauteile der Elektronikereinheit mit Energie versorgt. Zudem kann der Zündschlüssel **3** eine oder mehrere, nicht dargestellte Tasten aufweisen, bei deren Betätigung ein Codesignal in der Steuereinheit **4** erzeugt und über den Sender **6** ausgesendet wird.

Die ausgesendeten codierten Signale enthalten jeweils eine codierte Information (Codeinformation), die empfangenseitig mit einer erwarteten Codeinformation (Sollcodeinformation) verglichen wird. Nur bei – zumindest weitgehender – Übereinstimmung der beiden werden die in den Signalen enthaltenen Steuerbefehle ausgeführt.

An einer geeigneten Stelle im Kraftfahrzeug ist ein Emp-

fänger 11 angeordnet, der das Codesignal über seine Antenne 12 empfangen kann. Die Antenne 12 kann in einem Außenspiegel, am Innenspiegel oder an sonstiger, von Signalen von außerhalb und von innerhalb des Fahrzeugs einwandfrei erreichbarer Stelle angeordnet sein. Der Empfänger 11 weist eine Speichereinheit 13, insbesondere ein EEPROM, auf, in der eine Sollcodeinformation dauerhaft gespeichert ist. Sobald das Codesignal empfangen wird, wird die in ihm enthaltene Codeinformation mit der Sollcodeinformation verglichen. Bei Übereinstimmung der beiden werden ein Türschloß, alle Türschlösser und/oder das Kofferraumschloß ver- oder entriegelt.

Wenn der Benutzer in sein Fahrzeug eingestiegen ist und dann den Verbrennungsmotor starten möchte, so steckt er den Zündschlüssel 3 in ein Lenkrad- oder Zündschloß 14 und dreht den Zündschlüssel 3, wobei ein Zündschalter 15 betätigt wird. Infolgedessen wird eine Sende- und Empfangseinheit 16 am Zündschloß 14 aktiviert, die bei eingestecktem Zündschlüssel 3 über einen schloßseitigen Schwingkreis 10 mit einer Spule 18 und einem Kondensator mit dem schlüsselseitigen Schwingkreis 8 magnetisch gekoppelt ist. Infolgedessen wird ein Anforderungssignal induktiv zu dem Schwingkreis 8 auf dem Zündschlüssel 3 übertragen.

Der schlüsselseitige Schwingkreis 8 bildet zusammen mit der Steuereinheit 4 und dem Speicher 5 (RAM) einen Transponder. Der Transponder antwortet automatisch auf ein empfangenes Anforderungssignal mit einem Antwortcodesignal. Mit dem Antwortcodesignal versucht der Transponder seine Berechtigung nachzuweisen (Authentifikation).

Wenn die Sende- und Empfangseinheit 16 ein Antwortcodesignal empfängt, so wird die in dem Antwortcodesignal enthaltene Codeinformation mit einer erwarteten Sollcodeinformation verglichen. Bei Übereinstimmung (erfolgreiche Authentifikation) wird ein Freigabesignal erzeugt, durch das eine elektronische Wegfahrsperre 2 gelöst wird.

Falls eine elektronische Lenkungsverriegelung vorhanden ist, so kann diese ebenfalls durch das Antwortcodesignal oder durch das Codesignal entriegelt werden, damit das Lenkrad bewegt werden kann.

Die in dem Codesignal oder dem Antwortcodesignal enthaltene Codeinformation sowie die Sollcodeinformation können jeweils mit Hilfe eines mathematischen Algorithmus erzeugt werden. Der mathematische Algorithmus kann hardwaremäßig (als logische Schaltung) oder softwaremäßig auf dem Zündschlüssel 3 oder in der Sende- und Empfangseinheit 16 realisiert sein.

Eine Codeinformation, die in dem Codesignal von dem Zündschlüssel 3 zu dem Empfänger 11 zum Ver- oder Entriegeln übertragen wird, ist bei jedem Aussenden gegenüber der zuvor ausgesendeten Codeinformation verändert. Das Ändern geschieht dabei mit Hilfe des mathematischen Algorithmus innerhalb eines Zyklus (daher wird dies auch als Wechselcode oder Rolling Code bezeichnet). Bei jeder Neuberechnung wird von der zuvor empfangenen Codeinformation als Startwert ausgegangen. Die Länge des Zyklus, d. h. die Gesamtanzahl von möglichen, unterschiedlichen Codesignalen hängt von der Komplexität des Algorithmus und der Bitlänge der Codeinformation ab. Bei einem sicheren Diebstahlschutzsystem ist die Codeinformation zumindest 32 Bit lang. Die Zykluslänge ergibt sich dabei auf mehrere Milliarden unterschiedliche Codeinformationen.

Das Ändern der Codeinformation kann auch mit Hilfe eines sogenannten Kryptocodes vonstatten gehen. Dabei wird bei jeder Neuberechnung die zuvor empfangene Codeinformation als Startwert verwendet. Die empfangene Codeinformation ist zuvor als zufälliger Wert in der Sende- und Empfangseinheit 16 erzeugt worden. Zum Berechnen der neuen

Codeinformation wird ein geheimer Kryptoschlüssel sowohl schloßseitig als auch schlüsselseitig benötigt, der von außen nicht auslesbar und zugriffsgeschützt jeweils in einem Sicherheitsspeicher 17 (wie einem eigenen EEPROM) gespeichert ist.

Um eine Übereinstimmung mit der Sollcodeinformation zu erreichen ist also die Kenntnis der zuvor übermittelten Codeinformation zusammen mit dem Algorithmus notwendig. Infolgedessen können widerrechtlich abgehörte Codesignale allein nicht zum Entriegeln des Fahrzeugs benutzt werden, da beim nächsten Mal ein mit dem Algorithmus verändertes Codesignal erwartet wird.

Im Zündschlüssel 3 wird die zuletzt ausgesendete Codeinformation in dem Speicher 5 vorübergehend gespeichert, und zwar solange entweder noch kein neues Codesignal erzeugt wurde oder solange die Batterie 9 den Speicher 5 mit Energie versorgt. In der Speichereinheit 13 des Empfängers 11 wird die als berechtigt erkannte Codeinformation dauerhaft so lange gespeichert, bis eine neue Codeinformation als berechtigt erkannt und die alte Codeinformation überschrieben, gelöst oder ungültig wird.

Wenn der Energievorrat der Batterie 9 des Schlüssels 3 leer ist, so kennt der Zündschlüssel 3 nicht mehr die zuletzt gesendete Codeinformation. Der Empfänger 11 hingegen ermittelt die Sollcodeinformation ausgehend von seiner zuletzt als berechtigt erkannten Codeinformation. Falls in diesem Falle ein Codesignal nach ausgetauschter Batterie 9 zu dem Empfänger 11 gesendet wird, so wird die darin enthaltene Codeinformation mit größter Wahrscheinlichkeit nicht als berechtigt erkannt. Selbst ein gegebenenfalls vorhandener Synchronisationsbereich (begrenzte Anzahl von in dem Zyklus aufeinanderfolgenden Codeinformationen) kann in der Regel keine Synchronisation mehr herstellen.

Ein vorhandener Synchronisationsbereich hilft nur in dem Falle, wenn die Codeinformation des Schlüssels 3 durch "blindes" Betätigen des Schlüssels 3 lediglich um einige wenige Zyklusschritte weiter ist als die Sollcodeinformation im Empfänger 11.

Falls jedoch die Batterie 9 des Schlüssels 3 "leer" ist, so ist die gesamte Codeinformation des Schlüssels 3 verlorengegangen. Infolgedessen muß das Diebstahlschutzsystem neu initialisiert werden, damit sowohl im Zündschlüssel 3 als auch im Empfänger 11 die gleiche Codeinformation vorhanden ist, um das Codesignal zu erzeugen und die Zentralverriegelungsanlage 1 des Fahrzeugs fernbedient zu betätigen.

Das erfindungsgemäße Verfahren zum Initialisieren eines Diebstahlschutzsystems wird im folgenden anhand der Fig. 2 näher erläutert.

Zunächst muß der Benutzer in sein Fahrzeug einsteigen. Falls das Entriegeln der Fahrzeugtüren dabei nicht durch das Codesignal bewerkstelligt werden kann, weil die Batterie 9 des Zündschlüssels 3 leer war, so kann der Benutzer die Türen mit Hilfe des Barts des Zündschlüssels 3 mechanisch entriegeln. Zum Einleiten der Initialisierung steckt der Benutzer im Schritt S1 den Zündschlüssel 3 in das Zündschloß 14 und betätigt das Zündschloß 14 innerhalb einer vorgegebenen Zeitdauer unüblich. Dies kann ein zumindest drei- oder mehrmaliges, schnelles Hin- und Herdrehen des Schlüssels 3 innerhalb von z. B. 10 sek von der Ausgangsstellung in eine Endstellung und wieder zurück sein.

Das unübliche Betätigen (mehrfaches, hintereinanderfolgendes Verdrehen des Zündschlüssels) des Zündschlosses 14 soll deutlich unterscheidbar von dem üblichen Betätigen (Zündschlüssel ins Zündschloß 14 stecken und den Zündschlüssel 3 von der Ausgangsstellung in die Startstellung verdrehen) sein. Die Zeitdauer wird daher auch derart vorgegeben, daß ein Verwechseln mit dem unter Umständen

zweimaligen Betätigen des Zündschlüssels 3 beim fehlgeschlagenem Starten des Motors unterscheidbar ist. Das unübliche Betätigen wird daher sofort erkannt und das Diebstahlschutzsystem wird daraufhin in einen Initialisierungszustand versetzt. Nur in diesem Initialisierungszustand kann das Diebstahlschutzsystem initialisiert werden.

Der Zündschlüssel 3 sollte sich am Ende der Zeitdauer in einer Drehstellung befinden, in der der Zündschalter 15 eingeschaltet ist und somit eine elektrische Verbindung zwischen dem Pluspol der Fahrzeugbatterie (wird auch als Klemme 30 bezeichnet) und einer sogenannten Klemme R herstellt. In dieser Stellung werden sowohl der Empfänger 11 als auch die Sende- und Empfangseinheit 16 mit Energie (Bordnetzspannung) versorgt. Der Empfänger 11 und die Sende- und Empfangseinheit 16 können beispielsweise mit +12 V oder +24 V aus der Fahrzeugbatterie versorgt werden.

Infolge des mehrfachen Einschaltens (unübliches Betätigen) des Zündschalters 15 wird die Sende- und Empfangseinheit 16 angewiesen, im Schritt S2 einen Frage-Antwort-Dialog durchzuführen. Hierzu sendet die Sende- und Empfangseinheit 16 ein Anforderungssignal über ihre Spule zu dem Transponder im Zündschlüssel 3. Der Transponder kann dem Anforderungssignal soviel Energie entnehmen, wie zum Erzeugen des Antwortcodesignal benötigt wird.

Der Transponder erzeugt nach Empfang des Anforderungssignals ein codiertes Antwortcodesignal, das zurück zu der Sende- und Empfangseinheit 16 gesendet wird (dieser Vorgang der bidirektionalen Daten-/Energieübertragung wird als Frage-Antwort-Dialog FAD bezeichnet). Die Sende- und Empfangseinheit 16 überprüft im Schritt S3 die in dem Antwortcodesignal enthaltene Codeinformation auf ihre Berechtigung. Falls die empfangene Codeinformation als nicht berechtigt erkannt wird, so wird die Initialisierung abgebrochen, da davon auszugehen ist, daß ein Unberechtigter versucht, das Diebstahlschutzsystem zu initialisieren. Gegebenenfalls kann dann Alarm ausgelöst werden.

Wird das Antwortcodesignal hingegen als berechtigt erkannt, so wird im Schritt S4 ein Startwert zu dem Zündschlüssel 3 gesendet. Der Startwert stellt einen Anfangswert zum Berechnen der Codeinformation dar. Der Startwert wird von der Steuereinheit 4 empfangen und in den Speicher 5 (RAM) gespeichert, als ob er eine zuvor gesendete Codeinformation wäre.

Der Startwert wird anschließend im Schritt S5 über den Sender 6 zum Empfänger 11 gesendet, der diesen Startwert im Schritt S6 in seiner Speichereinheit 13 (EEPROM) abspeichert. Auch im Empfänger 11 wird der Startwert so behandelt, als ob er eine zuvor empfangene und als berechtigt erkannte Codeinformation wäre.

Somit ist sowohl im Zündschlüssel 3 als auch im Empfänger 11 der Startwert bekannt, von dem ausgehend das nächste gültige Codesignal mit Hilfe des mathematischen Algorithmus erzeugt werden kann.

Sobald der Startwert sowohl im RAM des Zündschlüssels 3 als auch im EEPROM des Empfängers 11 gespeichert ist, ist die Initialisierung erfolgreich beendet. Die erfolgreiche Initialisierung kann nun – durch den Empfänger 11 gesteuert – im Schritt S7 durch eine nicht dargestellte Rückmeldeeinheit im Kraftfahrzeug optisch oder akustisch angezeigt werden. Als Rückmeldeeinheit können dabei ohnehin vorhandene Anzeigeeinheiten im Fahrzeug, wie beispielsweise Blinker, Hupe, Lampen oder LED im Armaturenbrett u.ä. dienen.

Die Sende- und Empfangseinheit 16 braucht nur einmal nach der Herstellung initialisiert zu werden, jedoch später nicht mehr, da diese später bei jedem Frage-Antwort-Dialog selbst einen zufälligen Startwert erzeugt und diesen dem

Transponder durch das Anforderungssignal mitteilt. Aus dem Startwert wird dann sowohl im Transponder das Antwortcodesignal als auch in der Sende- und Empfangseinheit 16 die Sollcodeinformation erzeugt.

Die Sende- und Empfangseinheit 16 ist zusammen mit dem Zündschlüssel 3 erstmalig am Bandende beim Fahrzeughersteller initialisiert worden. Dort oder bereits beim Hersteller des Diebstahlschutzsystem wurde der mathematische Algorithmus in einen oder alle dem Fahrzeug zugeordneten Zündschlüsseln 3 sowie der Sende- und Empfangseinheit 16 implementiert. Dieser Algorithmus kann von einem Außenstehenden nicht "entschleiert" werden. Zusätzlich zu dem Algorithmus können auch fahrzeug- oder personenbezogenen Daten zum Erzeugen der Codeinformationen verwendet werden.

Die Sende- und Empfangseinheit 16 erzeugt bei jedem Aktivieren (Drehen des Zündschlüssels oder Einschalten eines Zündschalters) einen Zufallswert, der als Anforderungssignal oder als Startwert zum Zündschlüssel 3 übertragen wird. Mit Hilfe des Zufallswerts wird im Zündschlüssel 3 das Antwortsignal erzeugt. Da in der Sende- und Empfangseinheit 16 der Zufallswert ohnehin bekannt ist, kann daraus mit dem gleichen Algorithmus wie im Transponder die Sollcodeinformation erzeugt werden und mit der Codeinformation des Antwortsignals verglichen werden.

Der Speicher 5 im Zündschlüssel 3 ist als RAM ausgebildet. Da ein RAM beim Speichern von Daten weniger Energie verbraucht, wird durch Verwenden eines RAM die Lebensdauer der Batterie 9 verlängert. Der Benutzer braucht nicht so häufig die Batterie 9 auszutauschen, falls sie leer ist. Ein RAM hat zudem den Vorteil, daß bei Abschalten der Batteriespannung, zum Beispiel durch Herausnehmen der Batterie 9, die Daten im Speicher 5 verloren gehen. Somit kann ein Unberechtigter die Daten im RAM nicht mehr auslesen, um die zuletzt verwendete Codeinformation herauszubekommen. Ein Überlisten des Diebstahlschutzsystems wird somit erschwert. Zudem ist ein RAM ohnehin als Arbeitsspeicher für die Steuereinheit 4 vorhanden. Da auf die Daten oft zugegriffen wird, ist es vorteilhaft ein RAM zu verwenden, da dieser Datenzugriff weniger Energie verbraucht als beispielsweise ein Zugriff auf Daten in einem EEPROM.

Zusätzlich kann auch noch der Sicherheitsspeicher 17 vorhanden sein, in dem beispielsweise der geheime Kryptoschlüssel oder sonstige Daten, die dauerhaft gespeichert werden müssen, von außen nicht auslesbar gespeichert sind.

Die Steuereinheit 4 auf dem Zündschlüssel 3 steuert sowohl den Sender 6 als auch den Schwingkreis 8 des Transponders. Die Daten zum Erzeugen des Codesignals werden dem Speicher 5 (RAM oder bei einem Kryptocode sowohl RAM als auch dem zusätzlichen Sicherheitsspeicher 17) entnommen. Die Daten zum Erzeugen des Antwortcodesignals werden dem Transponder in dem Anforderungssignal mitgeteilt.

Die Signale, die bidirektional zwischen der Sende- und Empfangseinheit 16 und dem Transponder übertragen werden, werden induktiv übertragen. Hierzu ist auf beiden Seiten je ein Schwingkreis 8, 10 mit jeweils einer Spule 20 bzw. 18 und einem Kondensator 21 (schloßseitiger Kondensator ist nicht dargestellt) vorhanden. Der Schwingkreis 10 oder 8 wird durch eine hochfrequente Schwingung zum Schwingen angeregt, wodurch durch die Spule 18 bzw. 20 (Primärspule) ein Wechsellmagnetfeld erzeugt wird. Das Magnetfeld induziert dabei in der jeweils anderen Spule 20 bzw. 18 (Sekundärspule) eine Wechselspannung, in der die übertragene Codeinformation moduliert enthalten ist. Durch Demodulation wird diese Codeinformation zurückerhalten.

Falls die magnetische Kopplung zwischen den beiden



Spulen gut genug ist, so wird kein Schwingkreis benötigt. Die Daten können dann allein mit Hilfe eines Wechselmagnetfeldes, das durch einen durch die Primärspule fließenden Wechselstrom erzeugt wird, zu der Sekundärspule übertragen werden.

Statt induktiver, bidirektionaler Übertragung von Daten und Energie kann auch eine optische, bidirektionale Übertragung verwendet werden. Vorzugsweise findet die optische Übertragung im Infrarotbereich statt.

Das Codesignal wird zwischen dem Sender 6 und dem Empfänger 11 unidirektional und drahtlos übertragen. Vorteilhafterweise wird das Codesignal als Hochfrequenzsignal oder als optisches (Infrarot-)Signal übertragen. Allerdings muß der Empfänger 11 im Fahrzeug derart angeordnet sein, daß er das Codesignal (oder den Startwert) sowohl vom im Zündschloß 14 eingesteckten Zündschlüssel 3 als auch von außerhalb des Kraftfahrzeugs störungsfrei empfangen kann.

Das erfindungsgemäße Verfahren zum Initialisieren des Diebstahlschutzsystems erfolgt erfindungsgemäß mit erhöhter Sicherheit, da anstelle von nur mechanischer Codierung des Schlüsselbarts (beim Drehen im Zündschloß 14) die sichere Codierung durch ein empfangenes und als gültig erkanntes Antwortcodesignal in der Sende- und Empfangseinheit 16 verwendet wird. Das Diebstahlschutzsystem kann also nur dann initialisiert werden, wenn zuvor ein berechtigtes Antwortcodesignal von der Sende- und Empfangseinheit 16 empfangen wurde.

Der Startwert, der während der Initialisierung von dem Zündschlüssel 3 zum fahrzeugseitigen Empfänger 11 übertragen wird, wird sicher von dem Empfänger 11 empfangen, da sich der Zündschlüssel 3 während der Initialisierung in der Nähe des Empfängers 11 befindet. Eine Gefahr durch Abhören der Signalübertragung durch Fremde wird somit vermindert, da der rechtmäßige Benutzer während der Initialisierung anwesend ist. Außerdem kann vorgesehen sein, daß die Signalübertragung des Startwerts während der Initialisierung mit reduzierter Reichweite vonstattengeht.

Unter dem Begriff Initialisierung ist ein erstmaliges oder erneutes Vergeben eines Startwertes zum Erzeugen einer Codeinformation zu verstehen. Dabei wird die Codeinformation mit Hilfe eines mathematischen Algorithmus aus einer zyklischen Folge von Codeinformationen bei jedem Betätigen des Zündschlüssels 3 neu erzeugt. Der Startwert wird dabei sowohl im Zündschlüssel 3 als auch im Empfänger 11 aktualisiert. Typischerweise wird eine Initialisierung dann durchgeführt, wenn ein verlorengegangener Zündschlüssel 3 durch einen neuen ersetzt wird. Somit wird der alte Zündschlüssel 3 ungültig.

Vorzugsweise werden der Empfänger 11 und die Sende- und Empfangseinheit 16 bei der Erstinitialisierung am Bandende des Automobilherstellers durch ein besonderes Diagnosesignal in den Initialisierungszustand versetzt. Hierzu sendet ein von außerhalb an das Kraftfahrzeug anschließbares Gerät ein Initialisierungssignal über eine ohnehin vorhandene Diagnoseschnittstelle und eine Busleitung (Bordnetz) an den Empfänger 11 und die Sende- und Empfangseinheit 16. In diesem Falle braucht der Schlüssel 3 nicht unüblich in dem Zündschloß 14 betätigt zu werden, um die Initialisierung einzuleiten. Zu einem späteren Zeitpunkt kann die Initialisierung auch in autorisierten Fachwerkstätten durchgeführt werden, wenn diese mit einem entsprechenden Gerät ausgestattet und dazu auch berechtigt sind.

Das Codesignal kann auch Steuerinformationen enthalten, anhand derer der fahrzeugseitige Empfänger 11 erkennt, welche Funktionen im Kraftfahrzeug fernbedient werden sollen. Ein Steuern wird jedoch nur dann durchgeführt, wenn eine Authentifikation (überprüfen der Berechtigung) mittels der empfangenen Codeinformation erfolgreich statt-

gefunden hat. So können dann auch Fenster, Schiebedach, Verdeck, Sitze, Heizung, Klimaanlage, Lüftung, Spiegel, Alarmanlage usw. fernbedient gesteuert werden.

Die Steuereinheit 4 kann durch einen Mikroprozessor oder eine funktionell gleichwertige Einheit realisiert werden. In der Sende- und Empfangseinheit 16 kann ebenfalls ein Mikroprozessor vorhanden sein. Die Sende- und Empfangseinheit 16 kann in der Nähe des Zündschlosses 14 oder auch in einem ohnehin im Fahrzeug vorhandenen Steuergerät, wie dem Motorsteuergerät und/oder einem Bremssteuergerät und/oder einem Getriebesteuergerät, manipulationssicher untergebracht sein. Die Spule 18 der Sende- und Empfangseinheit 16 ist vorteilhafterweise am vorderen Ende des Zündschlosses 14 angeordnet, damit bei eingestecktem Zündschlüssel 3 eine gute magnetische Kopplung zu der Spule 20 auf dem Zündschlüssel 3 besteht.

#### Patentansprüche

1. Verfahren zum Initialisieren eines Diebstahlschutzsystems für ein Kraftfahrzeug, wobei das Diebstahlschutzsystem aufweist:

- einen Schlüssel (3), auf dem eine Fernbedieneinheit (4, 5, 6, 7) zum Ver- oder Entriegeln einer Zentralverriegelungsanlage (1) und ein Transponder (4, 5, 8) zum Lösen einer Wegfahrsperre (2) angeordnet sind,
- einen Empfänger (11) im Kraftfahrzeug, der Signale der Fernbedieneinheit (4, 5, 6, 7) empfängt und auswertet, und
- eine Sende- und Empfangseinheit (16) an einem Schloß (14), die ein Anforderungssignal zu dem Transponder (4, 5, 8) aussendet, ein codiertes Antwortsignal von dem Transponder empfängt und das Antwortsignal auf seine Berechtigung prüft,

**gekennzeichnet durch folgende Schritte:**

- Einleiten eines Initialisierungszustands, wodurch der Empfänger (11) und die Sende- und Empfangseinheit (16) in einen Initialisierungszustand versetzt werden,
- Aussenden des Anforderungssignals an den Transponder (4, 5, 8),
- Zurücksenden des Antwortsignals an die Sende- und Empfangseinheit (16),
- Überprüfen des Antwortsignals auf seine Berechtigung, indem eine in dem Antwortsignal enthaltene Codeinformation mit einer erwarteten und gespeicherten Sollcodeinformation verglichen wird,
- Aussenden eines codierten Startwertes an den Schlüssel (3), falls das Antwortsignal als berechtigt erkannt wurde, sowie Speichern des Startwertes in einem Speicher (5) des Schlüssels (3), und
- Weiterleiten des Startwertes vom Schlüssel (3) an den Empfänger (11).

**gekennzeichnet durch folgende Schritte:**

- Einleiten eines Initialisierungszustands, wodurch der Empfänger (11) und die Sende- und Empfangseinheit (16) in einen Initialisierungszustand versetzt werden,
- Aussenden des Anforderungssignals an den Transponder (4, 5, 8),
- Zurücksenden des Antwortsignals an die Sende- und Empfangseinheit (16),
- Überprüfen des Antwortsignals auf seine Berechtigung, indem eine in dem Antwortsignal enthaltene Codeinformation mit einer erwarteten und gespeicherten Sollcodeinformation verglichen wird,
- Aussenden eines codierten Startwertes an den Schlüssel (3), falls das Antwortsignal als berechtigt erkannt wurde, sowie Speichern des Startwertes in einem Speicher (5) des Schlüssels (3), und
- Weiterleiten des Startwertes vom Schlüssel (3) an den Empfänger (11).

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Startwert als Anfangswert zum Erzeugen eines codierten Fernbedienwechselcodesignals in einem Speicher (13) des Empfängers (11) gespeichert wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß eine erfolgreiche Initialisierung durch eine Anzeigeeinheit optisch und/oder akustisch angezeigt wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Signale zwischen dem Transponder (4, 5, 8) und der Sende- und Emp-

fangseinheit (16) als induktive oder optische Energie- oder Datensignale und die Signale von der Fernbedieneinheit (4, 5, 6, 7) zu dem Empfänger (11) als optische oder hochfrequente Datensignale übertragen werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Einleiten des Initialisierungszustands durch unübliches Betätigen des Schlüssels (3) in dem Schloß (14) innerhalb einer vorgegebenen Zeitdauer oder durch Anstecken eines externen Geräts an eine Diagnoseschnittstelle und Übertragen eines Initialisierungssignals vorgenommen wird, wodurch der Empfänger (11) und die Sende- und Empfangseinheit (16) in den Initialisierungszustand versetzt werden.

6. Diebstahlschutzsystem, das mit dem Verfahren nach Anspruch 1 initialisiert wird.

---

Hierzu 2 Seite(n) Zeichnungen

---

20

25

30

35

40

45

50

55

60

65







**FIG 2**

